Journal of Algebra **232,** 255–268 (2000)
doi:10.1006/jabr.2000.8399, available online at http://www.idealibrary.com on IDEAL®

Maximal Independent Generating Sets of the Symmetric Group

Julius Whiston

Communicated by Peter M. Neumann

Received December 2, 1999

1. INTRODUCTION

In a group, an *independent* set is a set of elements which satisfies the condition that no member of the set may be generated by the remaining elements of the set. The aim of this paper is to find the maximum size of any independent set in S_n. It is immediately evident that the set of transpositions $\{(1\,2), (2\,3), \ldots, (n-1\,n)\}$ forms an independent generating set of S_n and so the maximum size of an independent set in S_n is at least $n-1$. The purpose of this paper is to show that $n-1$ is an upper bound for the size of an independent set in S_n and that equality is only achieved when the set generates the whole of S_n.

This question was first posed by Diaconis and arose through the work of Holt and Rees [6] in their attempt to implement the Neumann–Praeger algorithm for finding which group is generated by a set of $n \times n$ matrices and in particular to examine typical elements of the group. The original algorithm was based on a random walk which started from the identity and at each step the current element was multiplied by a random element from the generating set; however, Holt and Rees were finding that the probability distribution of the resulting element took too long to approach the uniform distribution on all elements in the group. Holt and Rees suggested a new algorithm to fix this problem; Celler et al. [2] reported a dramatic increase in speed when the new algorithm was used. Given a group G with a generating set S, consider the complete directed graph on n vertices. Set $|S|$ of these vertices equal to each of the elements of S and the remaining ones to the identity. Then repeatedly pick a random edge (u, v) and

0021-8693/00 $35.00

replace the element at v with the element $g_u g_v$, where g_u and g_v are the elements at vertices u and v, respectively. This will generate an irreducible random walk through the set G^n. Diaconis and Saloff-Coste [4, p. 254] state that the random walk reaches an uniform distribution in time $|G|^{O(m(g))} n^2 \log n$, where $m(G)$ is the size of a maximal independent set in G. Thus an accurate bound for $m(G)$ would be desirable as a means of bounding the time for the algorithm.

It may also be of interest to note that this is related to the work done by Cameron et al. [1] in which they show that the maximum length of a chain of subgroups in S_n is $[\frac{3n-1}{2}] - b_n$, where b_n is the number of 1's in the binary expansion of n. In particular the bound on the maximal chain length of subgroups is a bound for the size of an independent set; however, from the result of this paper we can see that in general the maximal chain length is greater than the maximal size of an independent set.

2. PRELIMINARY DEFINITIONS

Let G act on Σ with $n = |\Sigma|$.

For a group I acting on a set Δ let $I_{(\Delta)} = \{g \in I : \delta g = \delta \text{ for all } \delta \in \Delta\}$ and $I^{\Delta} = I/I_{(\Delta)}$.

An *independent set*, S, is a set of elements of a group G such that for all g in S, g is not in $\langle S \setminus g \rangle$.

A *minimax set* for a group G is a largest independent set inside G.

Define $M(G)$ to be any minimax set of G with $m(G)$ as the size of $M(G)$.

3. BASIC STRATEGY

The theorem to be proved is:

THEOREM 1. *Given an independent set inside S_n, the size of the set is at most $n - 1$, with equality only if the set generates the whole group, S_n.*

In this paper, the approach for the proof is essentially inductive. If $n \leq 3$ the theorem obviously holds. The theorem is taken as true (by induction) on independent sets inside S_k for all $k \leq n - 1$. Then given an independent set of S_n, an element is removed to yield a group H. The element is chosen such that H is not the alternating group, A_n, which is always possible since if the group is A_n when an element is removed, the independent set contains even permutations and so removing one of those instead will yield a group with odd permutations and hence is non-alternat-

ing. If the group is intransitive or imprimitive then it is shown that the original set must have had size no more than $n - 1$ with equality only if the original group was the full symmetric S_n. Otherwise from the Aschbacher–O'Nan–Scott theorem it is deduced that the group must conform to one of a few types, each of which is examined individually to show that the original set was bounded accordingly. This proof is dependent upon the classification of finite groups to handle the case where H is an almost simple group.

Note that we establish in each case that either $m(H) \leq n - 3$ or else $m(H) = n - 2$ and when any independent element is added to $M(H)$, the group generated by the result is S_n. Thus we may conclude $m(A_n) \leq n - 2$.

Notation. Let H be the group resulting from the deletion of an element from an independent set of S_n.

4. CASE H IS INTRANSITIVE

If H is intransitive then Σ can be partitioned into Γ and Δ such that H acts on Γ and H acts on Δ. Let $I = H^{\Gamma}$, $J = H^{\Delta}$.

PROPOSITION 2. $m(H) \leq m(I) + m(J)$.

Proof. Given $M(H) = \{g_1, \ldots, g_l\}$, choose a subset $\{g_1, \ldots, g_k\}$ that is independent in its action on Γ and generates I. We shall produce a new minimax set for H, $\{h_1, \ldots, h_l\}$, with $\{h_{k+1}, \ldots, h_l\}$ fixing Γ pointwise.

For each i with $k + 1 \leq i \leq l$, if g_i has a non-trivial action on Γ then let w_i be an element in $\langle g_1, \ldots, g_k \rangle$ which inverts this action on Γ; otherwise set $w_i = 1$. Also, let $w_1 = 1$ for $i \leq k$.

Define a new set $\{h_1, \ldots, h_l\}$ by

$$h_j = \begin{cases} g_j, & j \leq k \\ g_j w_j, & j \geq k + 1. \end{cases}$$

Thus for $j \geq k + 1$, h_j fixes Γ.

We claim that $\{h_1, \ldots, h_l\}$ is an independent set.

Suppose not and that $h_i = h_{i_1}, \ldots, h_{i_m}$ with $i_j \neq i$.

If $i \leq k$ then consider the action on Γ; we may ignore h_s for $s \geq k + 1$ and so assume $i_j \leq k$.

This gives rise to an equality with respect to the action on Γ, $g_i = g_{i_1}, \ldots, g_{i_m}$.

This contracts the independence of $\{g_1, \ldots, g_k\}$ on Γ.

Otherwise, if $i \geq k + 1$ then replace each h_j with $g_j w_j$.

Thus, $g_i w_i = g_{i_1} w_{i_1} \cdots g_{i_m} w_{i_m}$.
Hence, $g_i = g_{i_1} w_{i_1} \cdots g_{i_m} w_{i_m} w_i^{-1}$.
Since g_i does not occur in any w_j, it does not occur on the right hand side.
Hence the equality contradicts the independence of $\{g_1, \ldots, g_l\}$.
Thus $\{h_1, \ldots, h_l\}$ is an independent set.
So we may assume that g_i is in $H_{(\Gamma)}$ for $k + 1 \leq i \leq l$.
Thus $m(J) \geq l - k$.
$m(H) = l = k + (l - k) \leq m(I) + m(J)$ as required. ∎

Thus

$$\begin{aligned} m(G) &= m(H) + 1 \leq m(I) + m(J) + 1 \\ &= (|\Gamma| - 1) + (|\Delta| - 1) + 1 \qquad \text{(by induction)} \\ &= |\Sigma| - 1. \end{aligned}$$

Hence if there is an element of $M(G)$ which can be deleted to give an intransitive group and the inductive hypothesis is true on groups acting on smaller sets, then $m(G) \leq n - 1$.
If $m(G) = n - 1$ then $m(I) = |\Gamma| - 1$ and $m(J) = |\Delta| - 1$; hence $I = S_\Gamma$ and $J = S_\Delta$ with $H \geq S_\Gamma \times S_\Delta$. If $|\Gamma| \neq |\Delta|$ then there are no proper overgroups of $I \times J$ in S_Σ and so $G = S_\Sigma$. If $|\Gamma| = |\Delta|$ then the only proper overgroup is $S_{|\Gamma|} \wr S_2$. However, by using the results of the next section, $m(S_{|\Gamma|} \wr S_2) \leq n - 2$ and so $G \neq S_{|\Gamma|} \wr S_2$, implying $G = S_n$.

5. CASE H IS TRANSITIVE BUT IMPRIMITIVE

If H is imprimitive then it can be embedded in a group $S_\Gamma \wr S_\Delta$ where $|\Gamma|, |\Delta| < |\Sigma|$ with $|\Sigma| = |\Gamma|.|\Delta|$.
Let $\Gamma_1, \ldots, \Gamma_u$ be the blocks, where $u = |\Delta|$ and write

$$J = H^\Delta,$$

and $g_1, \ldots, g_l$ as an independent generating set for H.

LEMMA 3. *It may be assumed that for some $k \leq |\Delta| - 1$, the elements $g_{k+1}, \ldots, g_l$ fix the blocks.*

Proof. Let $\{g_1, \ldots, g_k\}$ be an independent generating set for the block permutations so $J = \langle g_1^\Delta, \ldots, g_k^\Delta \rangle$.
Then, by induction, $k \leq |\Delta| - 1$.
We may use $g_1, \ldots, g_k$ to undo any block action in $g_{k+1}, \ldots, g_l$.
This preserves independence by an argument similar to before:

Suppose that for all $i \geq k+1$, the block action can be undone by $g_i \to g_i w_i$, where w_i is a word in $\langle g_1, \ldots, g_k \rangle$, and

$$\text{let } h_i = \begin{cases} g_i, & i \leq k \\ g_i w_i, & i \geq k+1. \end{cases}$$

Suppose that independence is not preserved and in particular $h_r = h_{i_1}, \ldots, h_{i_m}$ with $i_s \neq r$.

If $r \leq k$ then consider the block action. Since h_s^Δ is the identity for $s \geq k+1$, we may conclude $h_r^\Delta = h_{j_1}^\Delta \cdots h_{j_p}^\Delta$ with $j_t \leq k$.

Thus, $g_r^\Delta = g_{j_1}^\Delta \cdots g_{j_p}^\Delta$ with $j_t \leq k$ which contradicts the choice of $g_1, \ldots, g_k$.

If, instead, $r \geq k+1$ then $g_r = h_{i_1} \cdots h_{i_m} w_r^{-1}$.

Then g_r does not occur on the right hand side, thus contradicting the independence of $\{g_1, \ldots, g_l\}$.

Hence the lemma holds. ▮

PROPOSITION 4. *If $H \leq S_\Gamma \wr S_\Delta$ and $|\Gamma| \neq 2$ then $m(G) \leq |\Sigma| - 2$.*

Proof. Let $g_1, \ldots, g_k$ independently generate the full permutation action on the blocks, and let $g_{k+1}, \ldots, g_l$ fix the blocks with $k \leq |\Delta| - 1$ as in Lemma 3.

If there is no numbering of the blocks such that $g_{k+1}, \ldots, g_l$ acts as $S_{\Gamma_1} \times \cdots \times S_{\Gamma_{u-1}}$ on $\Gamma_1 \cup \cdots \cup \Gamma_{u-1}$ then $m(H) \leq |\Delta| - 1 + |\Delta|(|\Gamma| - 1) - 2 = |\Sigma| - 3$ and so $m(G) \leq |\Sigma| - 2$.

If $g_{k+1}, \ldots, g_l$ acts as $S_{\Gamma_1} \times \cdots \times S_{\Gamma_{u-1}}$ on $\Gamma_1 \cup \cdots \cup \Gamma_{u-1}$ then choose the smallest subset $\{g_{k+1}, \ldots, g_s\}$ which generates this action.

It is claimed that $l - k \leq |\Gamma| - 1 + u - 2$. Suppose $g_{k+1}, \ldots, g_r$ generates S_{Γ_1} without redundancy and for each $i \geq r+1$ we may form a word w_i in $g_1, \ldots, g_r$ such that $w_i g_i$ fixes the blocks setwise and fixes Γ_1 pointwise. Consider the group $\langle w_{r+1} g_{r+1}, \ldots, w_l g_l \rangle$; this fixes all the blocks setwise and Γ_1 pointwise. In particular, consider its action on Γ_2; one of the following situation will arise:

1. For, say, $i = r+1$, $w_i r_i$ is an odd permutation on Γ_2. In this case, we may form an element h_{12} from $g_1, \ldots, g_k$ that moves block 1 to block 2. If we allow $h_{12} g_{k+1} h_{12}^{-1}, \ldots, h_{12} g_r h_{12}^{-1}$ to act on $w_{r+1} g_{r+1}$ by conjugation, it is apparent that $\langle g_1, \ldots, g_{r+1} \rangle$ contains a group that fixes all the blocks setwise and acts as $S_{\Gamma_1} \times S_{\Gamma_2}$ on $\Gamma_1 \cup \Gamma_2$. Hence, for each $i \geq r+2$, there is a word, w_i, in $g_1, \ldots, g_{r+1}$ such that $w_i g_i$ fixes $\Gamma_1 \cup \Gamma_2$ pointwise.

2. $|\Gamma| \neq 4$ and for $i \geq r+1$ all the $w_i g_i$ are even permutations on Γ_2. By an analogous argument, we may conclude $\langle g_1, \ldots, g_{r+1} \rangle$ contains a group that fixes the blocks and acts as $(A_{\Gamma_1} \times A_{\Gamma_2}).2$ on $\Gamma_1 \cup \Gamma_2$. Thus for

each $i \geq r+2$, there is a word, w_i, in $g_1, \ldots, g_{r+1}$ such that $w_i g_i$ fixes $\Gamma_1 \cup \Gamma_2$ pointwise.

3. $|\Gamma| = 4$ and for $i \geq r+1$ all the $w_i g_i$ are even permutations on Γ_2 with some $w_j g_j$ being a 3 cycle. The same argument as in case 2 may be applied.

4. $|\Gamma| = 4$ and for $i \geq r+1$ all the $w_i g_i$ are 2^2 cycles. The same argument as in case 2 can be used except this time $\langle g_1, \ldots, g_{r+1} \rangle$ contains $(V_4 \times V_4) : S_3.2$ and this is sufficient to derive words w_i for $i \geq r+2$ such that $w_i g_i$ fixes $\Gamma_1 \cup \Gamma_2$ pointwise.

Thus the action of the base group of $\langle g_1, \ldots, g_l \rangle$ on $\Gamma_1 \cup \Gamma_2$ is the same as the action of the base group of $\langle g_1, \ldots, g_{r+1} \rangle$. By similar reasoning, it may be concluded that to generate the whole of the base group of H, only one element has to be added for each extra block. Thus:

$$m(H) \leq |\Delta| - 1 + |\Gamma| - 1 + |\Delta| - 1 = |\Gamma| + 2|\Delta| - 3.$$

If $|\Delta| \geq 3$ and $|\Gamma| \geq 3$ then $m(H) \leq |\Sigma| - 3$. Similarly if $|\Gamma| \geq 4$ then $m(H) \leq |\Sigma| - 3$. The case of $|\Delta| = 2$ and $|\Gamma| = 3$ is handled below. ∎

For the specific case of $H \leq S_3 \wr S_2$, we use the following lemma:

LEMMA 5. *If $H \leq S_3 \wr S_2$ then $m(G) \leq 5$ with equality only if $G = S_6$.*

Proof. First, it shall be assumed that $H = S_3 \wr S_2$ and hence $G = S_6$. If $m(H) \leq 4$ then there is nothing to prove. As $|H| = 2^3 3^2$, we know $m(H) \leq 5$. If $M(H)$ contains an element of order 4, say g_1, then $|\langle g_1 \rangle| = 4$ and so there can be, at most, three steps in the chain from $\langle g_1 \rangle$ to H which gives $m(H) \leq 4$. Hence it may be supposed that all elements have order 2 or 3 and that $M(H) = \{g_1, \ldots, g_5\}$. We may assume that g_1 swaps the blocks and $g_2, \ldots, g_5$ fixes the blocks setwise and so $g_1 = (14)(25)(36)$. Further, the group generated by any two elements, g_i and g_j, must have size $|g_i|.|g_j|$; in particular, none of the elements of $M(H)$ may be transpositions. If we apply an outer automorphism to G we would derive a new independent generating set for $S_3 \wr S_2$ with five elements which would contain a transposition contradicting the previous statement.

Suppose $H < S_3 \wr S_2$. If $m(H) = 3$ then there is nothing to do, so suppose $m(H) = 4$. Thus all the elements must have order 2 or 3 and so $g_1 = (14)(25)(36)$. The overgroup, G, must contain a transposition or 3 cycle by Sylow's theorem. Thus if the group is imprimitive it must be $S_3 \wr S_2$ which is not possible as $m(S_3 \wr S_2) \leq 4$. Hence the group is primitive and we must have $G = S_6$ with $m(G) = 5$. ∎

Now the case when $|\Gamma| = 2$ shall be considered.

PROPOSITION 6. *Suppose* $H \leq S_\Gamma \wr S_\Delta$ *and* $|\Gamma| = 2$; *then* $m(G) \leq |\Sigma| - 1$ *with equality only if* $G = S_\Sigma$.

Proof. Let $g_1, \ldots, g_k$ independently generate the full permutation action on the blocks and let $g_{k+1}, \ldots, g_l$ fix the blocks setwise with $k \leq |\Delta| - 1$. As before, let $u = |\Delta|$.

Consider the group $\langle g_{k+1}, \ldots, g_l \rangle$ as a subspace of a u dimensional vector space over F_2. $\{g_{k+1}, \ldots, g_l\}$ will be a basis for this subspace.

So $l - k \leq u$.

First, suppose that $k \leq u - 2$. If $|\{g_{k+1}, \ldots, g_l\}| \leq u - 1$ then $l = (l - k) + k \leq 2u - 3 = |\Sigma| - 3$. Thus $m(G) \leq |\Sigma| - 2$.

If $|\{g_{k+1}, \ldots, g_l\}| = u$ then $\langle g_{k+1}, \ldots, g_l \rangle$ is the full u dimensional space. For some i with $k + 1 \leq i \leq l$, $g_1 g_i g_1^{-1} \neq g_i$ for otherwise g_1 would fix every basis element and hence be the identity on the blocks. Since the field is F_2, we conclude that g_i and $g_1 g_i g_1^{-1}$ are linearly independent. The set $\{g_{k+1}, \ldots, g_l, g_1 g_i g_1^{-1}\}$ is not linearly independent and so some element other than g_i or $g_1 g_i g_1^{-1}$ may be removed; suppose this element is g_j. Thus we have $g_j \in \langle g_1, g_{k+1}, \ldots, g_{j-1}, \ldots, g_l \rangle$ which contradicts our assumption of independence.

Suppose that $k = u - 1$. Then $\langle g_1, \ldots, g_k \rangle$ generates the full symmetric group on Δ. At least one of $\langle g_1, \ldots, g_k, g_{k+1} \rangle$ or $\langle g_1, \ldots, g_k, g_{k+2} \rangle$ contains a subgroup which fixes all the blocks and is isomorphic to a subspace of codimension 1 in F_2^u. Hence either $\langle g_1, \ldots, g_{k+1} \rangle = S_2 \wr S_\Delta$ or $\langle g_1, \ldots, g_{k+1}, g_{k+2} \rangle = S_2 \wr S_\Delta$. This gives $|\{g_1, \ldots, g_l\}| \leq u - 1 + 2 = u + 1$. Since $S_2 \wr S_\Delta$ is maximal in S_Σ, we conclude $G = S_\Sigma$ and $m(G) \leq u + 2 \leq |\Sigma| - 1$ for $u \geq 3$. If $u = 2$ then $G \leq S_4$ which is handled in the following lemma. ∎

LEMMA 7. *If* $G \leq S_4$ *then* $m(G) \leq 3$ *with equality only if* $G = S_4$.

Proof. $|S_4| = 2^3 3$ and so $m(G) \leq 4$.

Suppose that $m(G) = 4$ or that $m(G) = 3$ and $G < S_4$; then g_i must all have order 2 or 3 and the group generated by any two, say g_i and g_j, must have order $|g_i|\,|g_j|$. If g_1 has order 3 then g_2 is a transposition and no other g_i is possible. So all the g_i are commuting involutions and, since they are independent, there are at most two. This is a contradiction. ∎

Henceforth, it shall be supposed that $n \geq 5$.

6. PRIMITIVE WREATH PRODUCT

If $H \leq I \wr J$ where I acts on r elements and J acts on s elements then H has a representation where it acts on r^s elements. We know H also has a faithful imprimitive representation where it acts on rs elements and that

$m(H) \leq rs - 2$. For $r \geq 3$ and $s \geq 2$ or $r \geq 2$ and $s \geq 3$, $rs < r^s$ and so $m(H) \leq r^s - 3$ which gives $m(G) \leq |\Sigma| - 2$.

7. USE OF THE ASCHBACHER–O'NAN–SCOTT THEOREM

By repeated use of the results for intransitivity and imprimitivity, the situation is reduced to the case where whatever element is deleted from the generating set of G, the resulting group, H, will be primitive and of the same degree as G. Thus the O'Nan–Scott theorem (see Dixon and Mortimer [5, Sect. 4.1]), which restricts the nature of H, is applicable:

THEOREM 8 (Aschbacher–O'Nan–Scott). *Let H be a finite primitive group of degree n, and let I be the socle of H. Then either*:

1. *I is a regular elementary Abelian p-group for some prime p, $n = p^m = |I|$, and H is isomorphic to a subgroup of the affine group $AGL_m(p)$; or*

2. *I is isomorphic to a direct power T^m of non-abelian simple group T and one of the following holds*:

   (a) *$m = 1$ and H is isomorphic to a subgroup of* $\mathrm{Aut}(T)$;

   (b) *$m \geq 2$ and H is a group of diagonal type with $n = |T|^{m-1}$*;

   (c) *$m \geq 2$ and for some proper divisor d of m and some primitive group U with a socle isomorphic to T^d, H is isomorphic to a subgroup of the wreath product $U \wr S_{m/d}$ with the product action, and $n = r^{m/d}$ where r is the degree of U*;

   (d) *$m \geq 6$, I is regular, and $n = |T|^m$.*

Consider the situations in which case 2(a) can arise and in particular when T might be the alternating group A_k. Due to the existence of an outer-automorphism on S_6, there are two cases to be considered, namely when $k \neq 6$ and when $k = 6$. In the former case, H is either A_k or S_k. However, as H has the same degree as G, we have $H = A_n$ and $G = S_n$. Thus some other element could be removed so that H is not a group consisting solely of even permutations. Note that this is always possible as this situation does not arise if $G = A_n$.

Now consider the latter case, i.e., when $k = 6$. The two situations that are not dealt with in the above are when $H = A_6.2 \neq S_6$ or $H = A_6.2^2$. From [3, p. 4], we can see that in these groups, the minimum degree of a permutation representation is 10. From Cameron et al. [1], we know the longest subgroup chain in S_6 has length $[\frac{3.6-1}{2}] - 2 = 6$. Hence the longest chain in A_6 has length 5. Thus the maximal chain length for $A_6.2^2$

is 7 which also serves as an upper bound for $m(A_6.2^2)$. So in this situation the theorem holds as $m(G) \leq 8$ and 10 is a lower bound for the degree of a permutation representation of G.

The primitive case 2(c) has already been handled. Case 2(d) gives rise to a twisted wreath product. The socle of this group is $(T)^m \leq (S_{|\Gamma|})^m$ and thus the group can be embedded $S_{|\Gamma|} \wr S_m$. Since $|\Gamma| < n$ and $m < n$, this situation is covered by case 2(c).

Each of the remaining cases will now be checked individually to show that $m(H)$ is less than $n - 3$ and thus $m(G)$ is less than $n - 2$.

8. CASE H IS A SUBGROUP OF $AGL_s(p)$

Consider the case where the resulting group H is either $AGL_s(p)$ or a primitive subgroup of $AGL_s(p)$.

We know that $|H| \leq p^{s^2+s}$ and so that the maximum chain length is bounded above by $(s^2 + s)\log_2 p$. The degree of the permutation representation is p^s. Thus if we show that $(s^2 + s)\log_2 p \leq p^s - 3$ then we would have shown that $m(G) \leq n - 2$.

Let $H_0 = H \cap GL_s(p)$ and let T be the set of translations inside H. There is a natural identification of T with the points of the vector space with the result that H is contained in $H_0 \ltimes T$.

PROPOSITION 9. *If H is a primitive subgroup of $AGL_s(p)$ then $m(G) \leq |\Sigma| - 2$.*

Proof. We know that for $s \geq 2$ and $p \geq 7$ with p prime, $(s^2 + s) \leq p^{s-1} - 1$. Hence in this domain, we have $(s^2 + s)\log_2 p \leq p^s - 3$ and thus $m(G) \leq n - 2$. Similarly, for $s \geq 4$ and $p \geq 3$, $(s^2 + s) \leq p^{s-1} - 1$, leading to the same conclusion.

For (s, p) taking values $(3, 5)$, $(3, 3)$, and $(2, 5)$, direct calculation of $(s^2 + s)\log_2 p$ and $p^s - 3$ shows that the inequality holds.

If $s = 2$ and $p = 3$ then $|AGL_2(3)| = 2^4.3^3$. Thus $m(AGL_2(3)) \leq 7$. As $AGL_2(3)$ is maximal in S_9, we conclude that the result holds for G if H is contained in $AGL_2(3)$.

If $p = 2$ then to establish $(s^2 + s)\log_2 p \leq p^s - 3$, it is sufficient to show $s^2 + s \leq 2^s - 3$. However, we know this holds for $s \geq 5$.

If $s = 4$ then we note that a length of a chain in $AGL_4(2) = 2^4.A_8$ is $4 + l(A_8) = 13$. Hence, if $H \leq AGL_4(2)$ then $m(H) \leq 13 \leq 2^4 - 3$.

For $s = 3$ and $p = 2$, see the following lemma. ∎

Thus we are just left with the case $AGL_3(2)$.

LEMMA 10. *If $H \leq AGL_3(2)$ and H is primitive then $m(G) \leq 6$.*

Proof. Suppose that H is a proper subgroup of $AGL_3(2)$; then H has to be either $2^3.7$ or $2^3.7.3$. Thus $m(H) \leq 5$ and so $m(G) \leq 6$.

Now, suppose that $H = AGL_3(2)$ with $g_1, \ldots, g_k$ a minimax set for H and consider the natural homomorphism to $GL_3(2)$. By looking at the possible chain lengths in $GL_3(2)$, we can see that at most four elements, $g_1, \ldots, g_4$, are required to generate a subgroup mapping surjectively onto $GL_3(2)$. As H is an affine group, the only proper normal subgroup of H is the set of translations, T. Thus $g_1, \ldots, g_4$ generates H or a subgroup isomorphic to $GL_3(2)$. In the former case, it can be concluded that $m(G) = 5$, whereas in the latter case, at most, only one more independent element inside $AGL_3(2)$ may be added to $g_1, \ldots, g_4$ since any subgroup $GL_3(2)$ is maximal in $AGL_3(2)$. Thus $m(G) \leq 6$. ∎

9. THE DIAGONAL CASE

Suppose T is a non-abelian simple group and H lies inside $(T \wr S_k)\text{Out}\, T < S_n$ with $n = |T|^{k-1}$.

To estimate Out T, we know that T has no more than $\log_2|T|$ generators and hence $|\text{Aut}\, T| \leq |T|^{\log_2|T|}$. This in turn gives $|(T \wr S_k)\text{Out}\, T| \leq |T|^k.k^k.|T|^{\log_2|T|}$. From this we derive

$$m(H) \leq k \log_2|T| + k \log_2 k + (\log_2|T|)^2.$$

If $k \geq 3$ then we have $m(H) \leq \log_2|T|.(k + |T|) + k^2 \leq |T|^{k-1} - 3$.
If $k = 2$ then $m(H) \leq 2\log_2|T| + (\log_2|T|)^2 + 2 \leq |T| - 3$.
Thus we see that $m(H) \leq n - 3$ and hence $m(G) \leq n - 2$.

10. AUTOMORPHISMS OF SIMPLE GROUPS

The situation where H is a subgroup of the automorphism group of a simple non-abelian group, T, is now considered. We show that the minimal degree of a permutation representation minus 3 is no less than an upper bound for the size of a maximal independent set. From this we conclude that $m(G) \leq n - 2$. First the simple classical groups will be considered, followed by the exceptional groups, and finally the sporadic groups. [7, Table 5.2.A] (with corrections for $P\Omega^+_{2m}(3)$ and $U_{6m}(3)$) will be used for establishing a lower bound for the minimal degree of the permutation representation of most of the classical groups. Further, the upper bounds for the sizes of the relevant automorphism groups are derived from [7, Tables 5.1.A–5.1.C].

Let $d(G)$ = the minimal degree of a permutation representation of G, and let $l(G)$ = the maximal chain length of G.

11. THE SIMPLE CLASSICAL GROUPS

11.1. *Linear Groups*

Let $T = L_m(q)$

It shall be initially assumed that $m \geq 3$.

We have $d(T) = (q^m - 1)/(q - 1)$ and $|H| \leq |\text{Aut } T| \leq 2q^{m^2}$ which gives $l(H) \leq \log_2 2q^{m^2} = m^2 \log_2 q + 1$.

Given that $(q^m - 1)/(q - 1) - 3 \geq m^2 \log_2 q + 1$ for $\{m \geq 3, q \geq 5\} \cup \{m = 4, q \geq 4\} \cup \{m \geq 5, q \geq 2\}$, it may be concluded that $d(H) - 3 \geq l(H)$ in this domain.

By calculating $|H|$ precisely, we verify that $d(H) - 3 \geq l(H)$ for $(m, q) = (3, 4), (3, 3), (4, 3)$.

If $(m, q) = (3, 2)$, from [3] it can be seen that the value of $m(L_3(2))$ is no more than 4 and that the minimal degree of a permutation representation of $L_3(2)$ is 7 and hence in this case $m(G) \leq 5 \leq n - 2$. Further, $m(\text{Aut } L_3(2))$ is no more than 5 and the minimal degree for a permutation representation of it is 8, so $m(G) \leq 6 \leq n - 2$.

Now we shall check the case when $m = 2$. It may be assumed that either $q \geq 11$ or $q = 8$.

For $m = 2$ and $q \geq 23$, $d(H) - 3 \geq q - 2 \geq 2^2 \log_2 q + 1 \geq l(G)$.

For $19 \geq q \geq 11$, the situation may be verified by direct calculation.

If $(m, q) = (2, 8)$ then from [3], longest chain has length 6 and the minimal degree of a permutation representation is 9.

It is concluded that $m(H) \leq d(H) - 3$ and thus $m(G) \leq n - 2$.

11.2. *The Symplectic Groups*

Let $T = PSp_{2m}(q)$

Noting that $PSp_2(q) \cong L_2(q)$ we need only consider $m \geq 2$.

If $m \geq 3$, $q \geq 3$ then $|H| \leq q^{2m^2+1+m}$ and $d(H) = (q^{2m} - 1)/(q - 1) \geq q^{2m-1} + 3$.

For $m \geq 3$ and $q \geq 3$, we have $d(H) - 3 = q^{2m-1} \geq (2m^2 + m + 1)\log_2 q \geq l(H)$.

If $q = 2$, $m \geq 3$ then $d(H) - 3 = 2^{2m-1} - 2^{m-1} - 3 \geq 2m^2 + m \geq l(H)$.

If $q \geq 3$, $m = 2$ then $|H| \leq 2q^{11}$ giving $d(H) - 3 \geq m(H)$.

If $q = m = 2$ then $PSp_4(2) \cong S_6$ which has already been handled.

From this it can be concluded that if T is symplectic then the theorem holds for G.

11.3. *Orthogonal Groups*

(i) $P\Omega_{2l+1}(q)$, $l \geq 3$, q *odd*. $|H| \leq q^{2(l^2+l)}$. If $q \geq 5$ then $d(H) = (q^{2l} - 1)/(q - 1)$, else if $q = 3$ then $d(H) = \frac{1}{2}3^m(3^m - 1)$. Hence $d(H) - 3 \geq 2(l^2 + 1)\log q \geq m(H)$.

(ii) $P\Omega^+_{2l}(q)$, $l \geq 4$. $|H| \leq 6q^{2l^2+1}$. For $q \neq 2$, $d(H) = (q^l - 1)(q^{l-1} + 1)/(q - 1)$ and for $q = 2$, $d(H) = 2^{l-1}(2^l - 1)$. Thus $d(H) - 3 \geq \log_2 6q^{2l^2+1} \geq m(H)$.

(iii) $P\Omega^-_{2l}(q)$, $l \geq 4$. $|H| \leq 2q^{2l^2+2}$ and $d(H) \geq q^{2l-3}$. If $q \geq 3$ and $l \geq 4$ or $q = 2$ and $l \geq 5$ then $d(H) - 3 \geq \log_2|\text{Aut } T| \geq m(H)$. It remains to check $d(H) - 3 \geq m(H)$ for the case when $q = 2$ and $l = 4$. If $q = 2$, $l = 4$ then $|\text{Aut } T| \leq 2^{12}.(2^4 - 1)(2^6 - 1)(2^4 + 1).2$. Thus $\log_2|\text{Aut } T| \leq 27$. Hence $d(H) \geq (2^4 + 1)(2^3 - 1) = 119 - 3 \geq \log_2|\text{Aut } T| \geq m(H)$.

11.4. *The Unitary Groups*

Let $T = U_n(q)$, $|H| \leq 2(q + 1)^{n^2}$.

(i) $n \geq 5$ and (n, q) is neither $(6m, 2)$ or $(6m, 3)$. $d(H) \geq (q^n - 1)(q^{n-1} - 1)/q^2$. Hence for $n \geq 5$, $d(H) - 3 \geq \log_2 \text{Aut } T \geq m(H)$.

(ii) $U_{6m}(3)$. $d(H) = \frac{1}{4}(3^n - 1)3^{n-1}$ where $n = 6m$. Since for $n \geq 6$, $\frac{1}{4}(3^n - 1)3^{n-1} - 3 \geq n^2 \log_2(3 + 1) + 1$, we conclude that $d(H) - 3 \geq m(H)$.

(iii) $U_{6m}(2)$. $d(H) = 2^{n-1}(2^n - 1)/3$ where $n = 6m$. Since for $n \geq 6$, $2^{n-1}(2^n - 1)/3 - 3 \geq n^2 \log_2(2 + 1) + 1$, we conclude that $d(H) - 3 \geq m(H)$.

(iv) $U_4(q)$. $d(H) = (q + 1)(q^3 + 1)$. Given $(q + 1)(q^3 + 1) - 3 \geq 16 \log_2 q + 1$, we conclude $d(H) - 3 \geq m(H)$.

(v) $U_3(q)$, $q \neq 2, 5$. $d(H) = q^3 + 1$. For $q \geq 4$, $q^3 + 1 - 3 \geq 9 \log_2 q + 1$ giving $d(H) - 3 \geq \log_2|\text{Aut } T| \geq m(H)$. If $q = 3$ then $q^3 = 27$, giving $|\text{Aut } T| = 2^6 3^3 7$ and hence $m(H) \leq \Omega = 11 < 27 - 2 = d(H) - 3$.

(vi) $U_3(2)$ is not simple.

(vii) $U_3(5)$. From [3], we have $d(H) = 50$. Since $|\text{Aut } T| = 2^5 3^3 5^3 7$, we have $\Omega = 12 < 47 = d(H) - 3$.

Thus if T is an unitary group then $m(G) \leq n - 2$.

12. THE EXCEPTIONAL GROUPS

In this section, [7, Table 5.1.B] is used to get a bound for the automorphism group and [7, Table 5.3.A] is used to get a bound for the degree of the minimal linear representation which is in turn a bound for the degree of the minimal permutation representation.

Group	$m(H) \leq$	$d(H) - 3 \geq$
$E_6(q)$	$80q$	q^9
$E_7(q)$	$134q$	q^{15}
$E_8(q)$	$249q$	q^{27}
${}^2E_6(q)$	$80(q+1)$	q^9
$F_4(q), q \geq 3$	$54q$	q^6
$F_4(2)$	54	64
$G_2(q), q \geq 5$	$16 \log_2 q$	$q^2(q-1)$
$G_2(4)$	32	413
$G_2(3)$	32	348
${}^2B_2(q) = Sz(q), q = 2^{2m+1}, m \geq 1$	$6 \log_2(q+1)$	$q^2 - 2$
${}^2G_2(q), q = 3^{2m+1}, m \geq 1$	$8 \log_2(q+1)$	$(q-1)^2$
${}^2F_4(q), q = 2^{2m+1}, m \geq 1$	$27 \log_2(q+1)$	q^4
${}^2F_4(2)$	18	1597
${}^3D_4(q), q \geq 3$	$33 \log_2 q$	$q^3(q^2-1) - 3$
${}^3D_4(2)$	20	21

In each case we can see that $m(H) \leq d(H) - 3$ and hence $m(G) \leq n - 2$.

13. THE SPORADIC GROUPS

Cameron et al. [1] give definite values of $l(H)$, the maximal length of a chain of subgroups for some of the Sporadic groups; of these the following values are used: M_i, J_{1-3}, HS, McL, Ru, Suz, $O'N$, Co_1, Fi_{22}, Ly. For M_{12}, M_{22}, J_2, J_3, Suz, McL, He, $O'N$, Fi_{22}, this value has to be increased by 1 to account for an outer automorphism.

This leaves J_4, He, Co_3, Co_2, Fi_{23}, Fi'_{24}, HN, Th, BM, M for which $l(H)$ is bounded by $\Omega(|H|)$.

For the degrees of the representation, [7, Proposition 5.3.8] is used to give a lower bound of $d(H)$ for the following groups: J_4, HS, McL, Ru, $O'N$, Fi_{22}, Fi_{23}, Fi'_{24}, HN, Ly, Th, BM, M.

For the remaining groups, namely M_i, J_1, J_2, J_3, He, Suz, Co_i, [3] is consulted to establish the index of the largest maximal subgroup.

H:	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	J_1	J_2	J_3	J_4	HS
$l(H) \leq$	7	9	11	11	14	6	11	11	34	12
$d(H) \geq$	11	12	22	23	24	266	100	6156	110	20

H:	McL	He	Ru	Suz	$O'N$	Co_3	Co_2	Co_1	Fi_{22}	Fi_{23}
$l(H) \leq$	13	21	17	18	14	23	30	26	22	38
$d(H) \geq$	21	2058	28	1782	31	276	2300	98280	27	234

H:	Fi'_{24}	HN	Ly	Th	BM	M
$l(H) \leq$	48	20	15	33	69	95
$d(H) \geq$	702	56	110	48	234	729

Since in each case, $l(H) \leq d(H) - 3$, we can deduce that $m(H) \leq d(H) - 3$ and hence $m(G) \leq n - 2$.

ACKNOWLEDGMENT

I thank my supervisor Jan Saxl for his extensive help in the preparation of this paper.

REFERENCES

1. P. J. Cameron, R. Solomon, and A. Turull, Chains of subgroups in symmetric groups, *J. Algebra* **127** (1989).
2. F. Celler et al., Generating random elements of a finite group, *Comm. Algebra* **23** (1995), 4831–4948.
3. J. H. Conway et al., "Atlas of Finite Groups," Clarendon, Oxford, 1985.
4. P. Diaconis and L. Saloff-Coste, Walks on generating sets of groups, *Invent. Math.* **134** (1998), 251–299.
5. J. D. Dixon and B. Mortimer, "Permutation Groups," Springer-Verlag, Berlin/New York, 1996.
6. D. Holt and S. Rees, An implementation of the Neumann–Praeger algorithm for the recognition of special linear groups, *J. Experiment. Math.* **1** (1992), 237–242.
7. P. Kleidman and M. Liebeck, "The Subgroup Structure of the Finite Simple Groups," Cambridge Univ. Press, Cambridge, UK, 1990.
8. P. M. Neumann and C. E. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc.* **65**, 555–603.